

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

FILED

OCT 22 2013

U. S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

one Samsung Galaxy Note II device, bearing serial/IMEI
#355429050603044, seized on October 8, 2013, and is currently in
the custody of the Drug Enforcement Administration, St. Louis
Field Office.

Case No. 4:13MJ00202 DDN

APPLICATION FOR A SEARCH WARRANT

I, Walter L. Holman, Jr., a federal law enforcement officer or an attorney for the government
request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:
*one Samsung Galaxy Note II device, bearing serial/IMEI #355429050603044, seized on October 8, 2013, and is
currently in the custody of the Drug Enforcement Administration, St. Louis Field Office,*

located in the EASTERN District of MISSOURI, there is now concealed

see attached LIST.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:


Code Section
Title 21 U.S.C. §§ 846 and 841(a)(1)

Offense Description
Conspiracy to possess with intent to distribute controlled
substance (heroin)

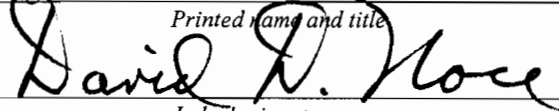
The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is
requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

WALTER L. HOLMAN, JR., Task Force Officer
Drug Enforcement Administration


Judge's signature

Sworn to before me and signed in my presence.

Date: October 22, 2013

City and State: St. Louis, MO

Honorable David D. Noce, U.S. Magistrate Judge
Printed name and title

AUSA: DEAN R. HOAG

LIST

1. All records on the target devices described as: (a) one Samsung Galaxy Note II device, bearing serial/IMEI #355429050603044 (hereafter referred to as "**subject cellular telephone #1**"); and (b) one Samsung Blackberry device, bearing serial/IMEI number #359782046255469 (hereafter referred to as "**subject cellular telephone #2**"), which relate to violations of Title 21, United States Code, Sections 846 and 841(a) (conspiracy to possess with the intent to distribute controlled substance) and involve MAURICIO DIAZ and/or his identified and unidentified co-conspirators, including:

- a. lists of customers and related identifying information;
- b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- c. any information related to sources of drugs (including names, addresses, telephone numbers, or any other identifying information);
- d. any information recording MAURICIO DIAZ or his identified and unidentified co-conspirator's schedules or travel to include any GPS data saved or stored on the devices to be searched;
- e. all bank records, checks, money orders, credit card bills, account information, and other financial records;
- f. images or video regarding the manufacture, distribution, or possession of controlled substances or any related financial transactions.

2. Evidence of user attribution showing who used or owned the target devices to be searched at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet to communicate via email, social media websites, or other electronic means, regarding customer purchases, shipments, financial transactions, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

5. All data files, including but not limited to, records and graphic representations, containing matter pertaining to the manufacture or trafficking in controlled substances or controlled substance analogs, that is, documents and visual depictions of accounting records, websites, marketing, and facilitating records.

6. Graphic interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI and MPEG) containing matter pertaining to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.

7. Electronic mail, chat logs, Internet Relay Chat (IRC) log files and electronic messages, concerning the trafficking of controlled substances and controlled substance analogs through interstate or foreign commerce, including by United States mail or by computer, visual depictions, and records pertaining to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.

8. Log files and other records concerning dates and times of connection to the Internet and to websites pertaining to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.

9. Any Instant Message conversations, chats, e-mails, text messages, or letters pertaining to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Walter L. Holman Jr., being duly sworn, depose and state:

I. INTRODUCTION

1. I am a Police Detective with the Lambert-St. Louis International Airport Police Department. I have been employed as a police officer with the Lambert-St. Louis International Airport Police Department for 17 years. Prior to that, I was employed for two years by the Pagedale Police Department as a police officer. I am currently assigned to the St. Louis Division of the Drug Enforcement Administration (DEA) as a Task Force Officer and have been so for approximately ten years. During my time as a law enforcement officer and my detachment with the DEA, I have conducted multiple narcotics-interdiction investigations and have participated in several complex investigations into drug trafficking organizations dealing in cocaine, heroin, MDMA or ecstasy, marijuana, and other controlled substances. I have also conducted surveillance, reviewed recorded illegal drug conversations and drug records, participated in undercover transactions, participated in court-authorized wiretaps and pen registers, served search and arrest warrants, and debriefed informants. Through my training, education and experience, I am familiar with the methods of operation of drug traffickers and the manner in which illegal drugs and bulk U.S. currency are transported, as well as the identification of controlled substances.

2. I have conducted investigations regarding computers, cellular telephones, and other related electronic storage devices and their use to commit and/or further crimes. I have been personally involved in the execution of search warrants to search residences and seize digital evidence, including computers, cellular telephones, and other related electronic storage devices. The information contained within this affidavit is either personally known to me or was provided to me by other law enforcement officers.

3. This affidavit is made in support of a search warrant for the following target devices:

a. one Samsung Galaxy Note II device, bearing serial/IMEI #355429050603044 (hereafter referred to as "**subject cellular telephone #1**"); and

b. one Samsung Blackberry device, bearing serial/IMEI number #359782046255469 (hereafter referred to as "**subject cellular telephone #2**"),

for evidence of the violations of Title 21, United States Code, Sections 846 and 841(a)(1) (Conspiracy to possess with intent to distribute a in excess of 100 grams of heroin, a Schedule I controlled substance). The target devices to be searched (**subject cellular telephones #1 and #2**) are currently in the lawful possession of the DEA. They came into the DEA investigators' possession in the following way: On October 8, 2013, DEA Task Force Group 33 executed a probable cause arrest of Mauricio DIAZ at the Phelps County Sheriff's Department, Rolla, Missouri. During the course of the arrest, DEA investigators seized the target devices (**subject cellular telephones #1 and #2**) which are the subject of this affidavit. The **subject cellular telephones #1 and #2** were subsequently transferred to the DEA Task Force Group 33 office. I am seeking this warrant out of an abundance of caution to be certain an examination of the target devices will comply with the Fourth Amendment and other applicable laws.

II. DEFINITIONS

4. The following definitions apply to this Affidavit:

a. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

b. "Computer hardware" consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, digital, magnetic, optical or similar computer impulses or data. Hardware includes any data-processing devices (such as central processing units and self-contained laptop or notebook computers or Personal Digital Assistants – PDAs); internal and peripheral storage devices (such as fixed disks, floppy disks, external hard disks, floppy disk drives and diskettes, tape drives and optical storage devices, thumb drives, and other memory storage devices).

c. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way the devices work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

d. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

e. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

g. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

5. The applied-for warrant would authorize the forensic examination of the devices for the purpose of identifying electronically stored data particularly described in the attached LIST. Because this affidavit is being submitted for the limited purpose of securing the requested search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause for the requested search warrant. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

III. INVESTIGATION BACKGROUND

6. On October 8, 2013, Phelps County, MO, Sheriff's Department Sgt. Carmelo Crivello conducted a traffic stop on westbound Interstate 44, at approximately mile marker 195, on a red 2006 Jeep Commander, bearing Texas license plate BKS-9191, registered to Oscar Gonzalez, 5710 Meadowbrook Drive 159, Ft. Worth, TX 76112.

7. Sgt. Crivello contacted the driver, who provided an Oklahoma operator's license, bearing the name Mauricio Alfredo DIAZ. Sgt. Crivello informed DIAZ of the reason for the stop. Sgt. Crivello engaged DIAZ in a conversation about his travels. DIAZ stated that he and his passenger, Erin LAGAN, traveled from Tulsa, Oklahoma, to Cleveland, Ohio, just to see the area and were traveling back home to Tulsa. Sgt. Crivello contacted the passenger, Erin LAGAN, who stated they had traveled to St. Louis to see the Gateway Arch. LAGAN stated that they had not traveled outside of St. Louis, Missouri. LAGAN was unable to provide any identification.

8. Due to the DIAZ's and LAGAN's conflicting stories about their travel, Sgt. Crivello asked DIAZ if he was transporting anything illegal to which DIAZ replied, "No." Sgt. Crivello asked DIAZ if he would consent to a search of the vehicle; DIAZ stated, "No." Sgt. Crivello requested a narcotics-trained detection canine to respond to his location for the purpose of conducting a search of the exterior of the vehicle. While awaiting the arrival of the canine unit, DIAZ admitted to smuggling heroin for a Mexican drug cartel. DIAZ stated the heroin he was transporting was under the driver's seat of the vehicle. DIAZ stated he went to Ohio to pick up the heroin for the cartels as a trial run. DIAZ stated that he recently picked up two kilograms of heroin in Denver,

Colorado, and was paid \$5,000 for the delivery. DIAZ informed Sgt. Crivello that he (DIAZ) wished to cooperate with law enforcement.

9. After a positive canine alert to the exterior of the vehicle, a search of the vehicle's interior revealed a glass pipe and an opened shrink-wrapped bag containing a brown rocky substance of approximately 181 grams of suspected heroin (Exhibit 1) under the center console. Sgt. Crivello asked DIAZ about the hole in the bag, and DIAZ stated that he had been instructed to sample the heroin on the way back to Tulsa, Oklahoma. Sgt. Crivello informed DIAZ that he found it hard to believe DIAZ would be transporting heroin for the cartels in that manner. DIAZ changed his story again by stating he was instructed to get a hotel room in Tulsa, sell the heroin, and send the money to Mexico.

10. Sgt. Crivello had DIAZ, LAGAN, and their vehicle transported to the Phelps County Sheriff's Department for further investigation.

11. A presumptive test of the contents in the plastic bag tested positive for heroin. Approximately 180 grams of heroin were seized. In my experience, 180 grams of heroin (slightly less than one half pound) is consistent with intent to distribute and not consistent with personal use.

12. Upon my arrival to the Phelps County Sheriff's Department, I advised DIAZ of his Miranda rights, and he signed a Form DEA-13, Advice of Rights, indicating his willingness to speak with the officers. DIAZ stated that he and LAGAN drove to Cleveland, Ohio, to pick up a package of heroin at a Wal-Mart parking lot to be delivered to an acquaintance named "Aleesha Green" in Tulsa, Oklahoma. DIAZ stated he was transporting the heroin in order to repay a bad drug debt he owed "Aleesha Green" and her boyfriend "Benny," who lives in Mexico. DIAZ stated part of the heroin he was transporting belonged to him, and he intended to sell the heroin out of a hotel room. DIAZ stated he is currently homeless and utilizes hotel rooms. DIAZ stated after he had sold his portion of the heroin, he would mail the money he owed to "Benny" in Mexico and keep what was left as his payment for transporting the drugs.

13. In an interview with LAGAN, she stated she was asked by DIAZ to travel to Cleveland, Ohio, to keep him company while he did a favor for a friend and was planning to see sites like the Gateway Arch.

14. Throughout the initial investigation and interviews with DIAZ and LAGAN, DIAZ received multiple phone calls and text messages on the **subject cellular telephones #1 and #2** from “Aleesha” and other numbers which DIAZ stated were from Mexico and were likely from “Benny.”

IV. DIGITAL EVIDENCE

15. Based on my knowledge, training, and experience, as well as that of agents and investigators with specialized training and experience in digital evidence and forensics, I am aware of the following considerations:

Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of crime, contraband, instrumentalities of crime, and/or fruits of crime. Digital and electronic files may be contraband, evidence, instrumentalities, or fruits of crime. Further, the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in various forms of electronic data.

16. Based on my knowledge, training, and experience, as well as that of agents and investigators with specialized training and experience in digital evidence and forensics, I am aware computer and digital files, or remnants of such files, can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten.

17. As used herein, the Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user typically subscribes to an access provider (also referred to as an internet service provider or “ISP”), which operates a host computer

system providing access to the Internet. Users can also access the Internet, using their own computer, but another person's or business's ISP. For example, a person can access the Internet at a large number of free, wireless access points, such as those provided at coffee shops or hotels.

18. Using a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including a modem (including dial-up connections and cable modems), a digital subscriber line (commonly referred to as a “DSL” connection), local area networks, wireless means, and numerous other methods.

19. As used herein, electronic mail (“e-mail”) is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends e-mail, it is typically initiated at the user’s computer, transmitted to a mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means. Similarly, people can also communicate using a variety of other means, such as instant messaging and text messaging.

V. CELLULAR AND MOBILE PHONES

20. As used herein, a cellular telephone or mobile telephone is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called “cells,” enabling communication with other cellular telephones or traditional “land line” telephones. A cellular telephone usually includes a “call log,” which records the telephone number, date, and time of calls made to and from the telephone.

21. In addition to enabling voice communications, typically cellular telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: receiving and storing voice mail messages, storing names and telephone numbers in electronic “address books;” sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet.

Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

22. A Samsung Galaxy Note II and a Samsung Blackberry are types of handheld wireless electronic communication devices known as smart phones from Samsung. Smart phones generally provide a wide range of applications. Among other things, Smart phones enable users to send email, make and receive telephone calls; access the Internet, take pictures, send instant / text messages, store and play digital music or video files. Additionally, data on a smart phone is typically synchronized to the smart phone user's computer system through a data cable. Such synchronized data can include call logs, text messages, GPS location data, photographs, and application data. Further, some of the same smart phone data can also be synchronized over the Internet using features commonly known as "Clouds," or a service provided by Google named "Google Drive." I have been advised analyzing a smart phone requires an examiner with specialized forensic training.

VI. TRAINING EXPERIENCE OF INVESTIGATIVE TEAM

23. With my experience and training, and that of other task force officers and special agents on the investigating team, based upon our training, experience, and participation in investigations involving the manufacture and distribution of controlled substances through the Drug Enforcement Administration, my investigation into controlled substances, from speaking with other agents and officers, and our investigation further detailed in this affidavit, we have learned the following:

a. Drug trafficking is traditionally a cash intensive enterprise due to its illicit nature, the desire to avoid records of sales, and the complexities of introducing this cash into the financial system. Persons involved in drug trafficking will often hold large amounts of cash on hand in their businesses and residences.

b. Persons involved in drug trafficking rely heavily on mobile telephones to conduct activities related to and in furtherance of the criminal activity. Mobile telephones are used to pass communications, such as instructions, negotiations, directions, and locations, both verbally and in writing via electronic message.

c. Persons involved in the distribution of controlled substances will disguise the distribution through a business operation and maintain business records,

including but not limited to telephone records and financial statements. I also know from my experience and training, as well as from discussions I have had with other law enforcement officers, that such records and documents are kept and stored in computers and electronic-memory devices in addition to or in lieu of hard-copy versions of this data. Similar to filing cabinets, boxes, or other physical devices for such records and documents, computers, electronic storage media and peripherals are commonplace and are often located inside residences. Further, documents and records can be "hidden" within such electronic storage media. Based on my knowledge, training, and experience, and the knowledge, training and experience of the investigators with expertise in computer and electronic/digital evidence, I am aware of the following search considerations and factors:

24. Volume of evidence: Computer storage devices, including but not limited to hard disks, diskettes, tapes, CDs, DVDs, and thumb drives, can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instruments of a crime. This sorting process can take weeks or months, depending on the volume of data stored.

25. Technical requirements: Searching computer systems for criminal evidence can be a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap") a controlled environment is essential to its complete and accurate analysis.

26. Data analysts may use several different techniques to search electronic data for evidence or instrumentalities of a crime. These include, but are not limited to the

following: examining file directories and subdirectories for the lists of files they contain, "opening" or reading the first few "pages" of selected files to determine their contents, scanning for deleted or hidden data, searching for key words or phrases ("string searches"). In view of the forgoing, computer-related items sought to be searched include the following:

a. Hardware - Computer hardware consists of any and all computer equipment capable of being linked together in a local area network (LAN) (to include any equipment which has remote access capabilities), including all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes, but is not limited to, any data-processing devices (such as central processing units, and self-contained laptop or notebook computers); internal and peripheral storage devices (such as hard drives, fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, flash drives, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communication devices (such as modems, cables, and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks);

b. Software - Computer software is digital information which can be interpreted by a computer and any related components to direct the way they work. Software is stored in electronic, magnetic, optical, or digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs;

c. Documentation - Computer related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related item;

d. Mobile devices - advances in mobile technology, such as "smart" phones, have made it possible for persons or representatives of businesses and criminal organizations to conduct activities on personal mobile devices, such as telephones, or personal electronic tablet devices, such as an iPad, which are capable of sending electronic communications including electronic mail and electronic "text" messages.

These devices also make it possible for an individual to access the Internet to operate email, websites, or store digital and electronic information;

e. Electronically Store Data - Any and all such data concerning the sales of imitation controlled substances and drug paraphernalia, laundering of monetary instruments, and engaging in monetary transactions in property derived from specified unlawful activity. Any and all identification documents and such data consisting of information stored on back-up tapes, computer hard drives, and/or any other form or manner;

f. Passwords and Data Security - Computer passwords and other data security devices are designated to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming codes. A password (a string of alphanumeric characters) usually operates as a sort of digital key to "unlock" particular data security devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

VII. COMPUTER EXAMINATION METHODOLOGY TO BE EMPLOYED

27. The examination procedure of electronic data contained in computer hardware, cellular telephones, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other examination procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully

possessed, or (5) evidence of the offenses specified above);

- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to

determine whether occurrences of language contained in such storage areas exist that are likely to appear in the **subject cellular telephones #1 and #2**; and/or performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in the attached LIST.

VIII. CONCLUSION

28. The digital media to be searched will be examined by one or more agents or law enforcement officers and technicians with specialized forensic training. In examining the cellular / mobile telephones identified herein, all searches will be limited to the device itself – the search will not involve contacting the service provider for the telephone to download information from the service provider to the device (e.g., voice mail or text messages that have not yet been delivered from the service provider to the device).

29. Searching the digital media to be searched for the evidence described in paragraph two will require a range of computer forensic analysis techniques. Criminals can mislabel or hide files and directories; encode communications to avoid using key words; attempt to delete files to evade detection; or take other steps designed to frustrate law enforcement searches for information. In order to properly execute the search authorized by the warrant, specially trained agents or forensic analysts will be required to conduct a thorough forensic analysis of the seized media, such as scanning areas of the disk not allocated to listed files, or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, I request permission to use whatever computer forensic analysis techniques appear necessary to locate and retrieve the evidence described in paragraph two.

30. Due to the fact that the digital media to be searched has already been seized pursuant to lawful procedures, and due to the potential volume of information, complexity, and variety of items to be searched, it will not be possible to complete a full

analysis of the digital media to be searched within ten (10) days. Accordingly, I request the Court's permission to provide a return that indicates when the digital media to be searched has been submitted for forensic evaluation.

31. In view of the foregoing, there is probable cause to conclude that, in the digital media to be searched within **subject cellular telephones #1 and #2**, there will be located evidence of a crime, contraband, the fruit or instrumentalities of a crime, of one or more violations of Title 21, United States Code, Section 841(a) and 846 (unlawful manufacture, distribution, or possession with intent to distribute a controlled substance and conspiracy). Accordingly, I respectfully request the issuance of a warrant to search the target devices (**subject cellular telephones #1 and #2**) for the items described in the attached LIST.